2020년05월30일년 정보보안기사 필기시험 기출문제 답안

【1과목 : 20문제】 시스템 보안	1	2	3	4	5	6	7	8	9	10
	④	①	④	③	①	②	①	④	③	①
	11	12	13	14	15	16	17	18	19	20
	②	①	②	①	②	②	③	④	②	②

【2과목 : 20문제】 네트워크 보안	21	22	23	24	25	26	27	28	29	30
	①	②	③	④	②	①	③	③	③	①
	31	32	33	34	35	36	37	38	39	40
	④	③	③	②	④	②	①	①	③	④

【3과목 : 20문제】 어플리케이션 보안	41	42	43	44	45	46	47	48	49	50
	③	④	①	④	①	②	④	②	①	①
	51	52	53	54	55	56	57	58	59	60
	③	④	④	④	④	③	②	④	④	④

【4과목 : 20문제】 정보 보안 일반	61	62	63	64	65	66	67	68	69	70
	①	④	④	②	④	①	③	①	④	③
	71	72	73	74	75	76	77	78	79	80
	④	④	③	④	④	④	④	①	④	④

【5과목 : 20문제】 정보보안 관리 및 법규	81	82	83	84	85	86	87	88	89	90
	①	④	④	①	④	④	④	④	④	④
	91	92	93	94	95	96	97	98	99	100
	③	④	③	④	③	①	①	④	①	④

전자문제집 CBT 홈페이지 : https://www.cbtestpro.kr

최신 수정 자료와 해설(오타・오답・규정변경)은 cbtestpro.kr 웹 및 앱에서 확인하세요.

기출문제의 저작권은 출제기관에 있습니다. cbtestpro.kr 및 관련 앱에서는 편집 및 재구성 작업만 하였음을 밝힙니다.



전자문제집 CBT

빠르고 효과적으로 배워 시험 합격을 노려라!

Download on the App Store

GET IT ON Google Play

【1과목】 시스템 보안 (20문제)

1. 리눅스 서버에서 xinetd 데몬을 이용한 접근 제어 시 지정된 원격지 IP 주소 대역에 대해 접근을 허락할 때 xinetd.conf 파일에서 사용하는 옵션은?

① enable
② allow
③ enable_access
❹ only_from

2. i-node가 가지고 있지 않은 정보는?

❶ 파일 이름
② 파일의 링크 수
③ 파일 크기
④ 마지막으로 수정된 시간

3. /etc/shadow 파일의 일부분이다. 이를 통해 알 수 있는 내용이 아닌 것은?

```
sys_admin:!!:15265:0:99999:7:0:11423:
sec_admin:$1$Elnjin$Excskscumink:15860:0:30:10:::
prog_user:$1$LFNJHS$gGkssceeskekks:15711:3:30:
7::18108:
```

① sec_admin 사용자는 비밀번호 변경 후 최대 30일간 이를 사용할 수 있다.
② sys_admin 사용자의 비밀번호는 아직 부여되지 않은 상태이며, 계정은 막혀 있다.
③ prog_user 사용자는 비밀번호 유효기간이 만료되기 7일 전부터 비밀번호 만료에 관한 경고메시지를 받는다.
❹ prog_user 사용자는 비밀번호를 변경한 후 3일 이내에 자신의 비밀번호를 변경할 수 있다.

4. 파일 시스템이란 운영체제가 파일을 시스템의 디스크 상에 구성하는 방식을 말한다. 운영체제는 시스템의 디스크 파티션 상에 파일들을 일정한 규칙을 가지고 저장하는데 파일 시스템은 이러한 규칙들의 방식을 제시하는 역할을 한다. 다음 중 윈도우 운영체제에서 사용하는 파일 시스템이 아닌 것은?

① FAT16
② FAT32
❸ EXT3
④ NTFS

5. 좀비 프로세스를 확인하고 중지시키기 위한 UNIX 명령어에 대한 설명으로 올바른 것은?

❶ ps 명령어 실행 후 STAT 값이 Z로 표시되는 프로세스가 좀비 프로세스이며, kill 명령어 사용
② ss 명령어 실행 후 STAT 값이 B로 표시되는 프로세스가 좀비 프로세스이며, kill 명령어 사용
③ ps 명령어 실행 후 STAT 값이 B로 표시되는 프로세스가 좀비 프로세스이며, halt 명령어 사용
④ zs 명령어 실행 후 STAT 값이 Z로 표시되는 프로세스가 좀비 프로세스이며, halt 명령어 사용

6. 매일 오전 8시 40분에 /usr/logreport.sh 스크립트가 실행되도록 하기 위해 contab에 넣을 설정 내용으로서 적절한 것은?

① * 40 08 * * -exec {/usr/logreport.sh}
❷ 40 08 * * * /usr/logreport.sh
③ * * * 08 40 /usr/logreport.sh
④ * * * 08 40 –exec {/usr/logreport.sh}

7. 다음 지문에서 설명하는 유닉스 시스템 관리자용 명령어는?

슈퍼 블록에서 카운트하고 있는 마운트 된 파일 시스템, 디렉터리에서 사용 가능한 디스크 블록과 free node 수를 알려 줌

❶ df
② ps
③ file
④ find

8. 다음 중 버퍼 오버플로우(Buffer Overflow)에 대한 대책으로 옳지 않은 것은?

① 경계 검사를 하는 컴파일러 및 링크를 사용한다.
② 경계를 검사하는 함수를 사용한다.
③ 운영체제 커널 패치를 실시한다.
❹ 최대 권한으로 프로그램을 실행한다.

9. 하이퍼바이저에 대한 내용으로 옳지 않은 것은?

① 가상머신과 하드웨어 사이에 위치하여 다수의 가상머신들이 각각의 운영체제가 구동될 수 있도록 논리적으로 독립된 가상머신 환경을 제공한다.

② 주 기능은 CPU, 메모리 등 하드웨어 자원을 각 가상머신에 논리적으로 분할 할당 · 스케줄링하는 것이다.

❸ 하이퍼바이저는 bare-metal 타입, hosted 타입으로 나누어지며, bare-metal 타입은 하드웨어 상에서 동작하는 것이 아니라 호스트 운영체제 위에서 동작한다.

④ hosted 타입은 VMware Workstation, Parallels Desktop 등이 대표적이다.

10. 다음 중 리눅스에서 Process ID(PID) 1번을 가지고 있는 프로세스는 무엇인가?

❶ init

② 부트로더

③ OS 커널

④ BIOS

11. 다음 지문이 설명하는 것은?

> 인터넷 애플리케이션에서 사용자 인증에 사용되는 공개 API(OpenAPI)로 구현된 표준 인증 방법이다. 트위터, 페이스북과 같은 SNS 서비스를 다른 애플리케이션 또는 다른 기기(PC, 스마트폰 등)에서 사용자 정보에 접근할 때 사용할 수 있도록 한다.

① Kerberos

❷ OAuth

③ EAP

④ RADIUS

12. 윈도우 NTFS에서 모든 파일들과 디렉터리에 대한 정보를 포함하고 있는 것은?

❶ MFT(Master File Table)

② FAT(File Allocation Table)

③ $AttrDef

④ $LogFile

13. 리눅스 시스템의 /etc/logrotate/conf 파일에서 로그순환 설정을 하려고 한다. 최소 6개월분의 로그를 저장하기 위해 빈칸 ㉠에 들어갈 용어로 적절한 것은?

```
/etc/logrotate.conf
monthly
( ㉠ ) 6
create
compress
include /etc/logrotate.d
```

① save

❷ rotate

③ cycle

④ minimum

14. FTP 접속기록을 확인할 수 있는 파일은?

❶ xferlog

② ftplog

③ error log

④ pacct

15. 다음 지문에서 설명하고 있는 것은?

> 리빙스턴사(루슨트에 인수)가 개발한 분산 보안 시스템(인증 프로토콜)이다. 통상적으로 ISP에서 사용하는 전화 등에 의한 원격 접속에 대한 인증용 서버를 지칭한다. 분산형 클라이언트/서버 기반의 동작으로 사용자 관리는 중앙집중식으로 수행한다. 인증방법은 PAP, CHAP 등 다양한 방법을 지원한다.

① S/Key 인증

❷ RADIUS

③ Challenge Response

④ Kerberos

16. 다음은 윈도우 부팅 순서이다. 올바르게 나열된 것은?

> 가. MBR - 부팅 매체에 대한 기본적인 파일시스템 정보를 읽는다.
> 나. POST - 하드웨어 자체의 시스템에 문제가 없는지 체크한다.
> 다. NTLDR - 하드디스크 부팅 파티션에 있는 프로그램으로 윈도우가 부팅될 수 있도록 간단한 파일시스템을 실행하며, BOOT.INI 파일의 내용을 읽는다.
> 라. NTDETECT.COM - 설치된 하드웨어를 검사한다.
> 마. NTOSKRNL.EXE - HAL.dll을 로드한다.
> 바. CMOS - 사용자가 설정한 기본사항을 읽어 시스템에 적용한다.

① 바-다-라-가-마-나
❷ 나-바-가-다-라-마
③ 나-바-다-라-가-마
④ 바-가-마-나-다-라

17. Cyber Kill Chain의 단계 중 빈칸 ⓐ, ⓑ에 들어갈 절차로 알맞은 것은?

> ① 정찰(Reconnaissance)
> ② 무기화(Weaponization)
> ③ (ⓐ)
> ④ 취약점 악용(Exploitation)
> ⑤ 설치(Installation)
> ⑥ (ⓑ)
> ⑦ 목표실행(Action)

① ⓐ 악성코드 제작(Develop) ⓑ 명령 및 제어(Command & Control)
② ⓐ 명령 및 제어(Command & Control) ⓑ 전달(Delivery)
❸ ⓐ 전달(Delivery) ⓑ 명령 및 제어(Command & Control)
④ ⓐ 전달(Delivery) ⓑ 악성코드 제작(Develop)

18. 다음 지문이 설명하는 것은?

> 감염 시스템의 리소스를 이용해 가상화폐를 채굴하여 공격자에게 전송하는 사이버 공격을 의미한다.

① CryptoCurrency Hijacking
② CryptoCurrency Jacking
③ Currency Hijacking
❹ CryptoJacking

19. 실행 레벨은 0부터 6까지 있는데 다음 지문의 빈칸 ㉠, ㉡, ㉢에 해당되는 실행 레벨로 알맞게 짝지어진 것은?

> ㉠ 단일 사용자 모드(Single User Mode)
> ㉡ 재부팅(Reboot)
> ㉢ 전체 서비스를 지원하는 다중 사용자 모드(Full Multiuser Mode)

① ㉠ 실행레벨 0 ㉡ 실행레벨 5 ㉢ 실행레벨 4
❷ ㉠ 실행레벨 1 ㉡ 실행레벨 6 ㉢ 실행레벨 3
③ ㉠ 실행레벨 0 ㉡ 실행레벨 5 ㉢ 실행레벨 3
④ ㉠ 실행레벨 1 ㉡ 실행레벨 6 ㉢ 실행레벨 2

20. 유닉스 또는 리눅스 시스템에서 SetUID와 SetGID가 설정된 모든 파일을 찾으려고 한다. 명령어가 바르게 기술된 것은?

① find / -type f ＼(-perm –1000 –o –perm -2000＼) -print
❷ find / -type f ＼(-perm -2000 –o –perm -4000＼) -print
③ find / -type f ＼(-perm -100 –o –perm -200＼) -print
④ find / -type f ＼(-perm -200 –o –perm -400＼) -print

【2과목】 네트워크 보안 (20문제)

21. Smurf 공격을 방지하기 위하여 라우터에서 차단되어야 하는 기능은?

❶ Directed Broadcast
② Ingress Filtering
③ HTTP GET Flooding
④ ICMP Ping Request

22. IPv4의 IP 주소 고갈 및 라우팅 테이블 대형화에 대한 해소책으로 기존의 클래스 기반 IP 주소 체계를 벗어나 서브넷 마스크 정보를 IP 주소와 함께 라우팅 정보로 사용할 수 있게 만든 IP 주소 지정 방식은?

① FLSM
❷ CIDR
③ VLSM
④ Static Routing

23. 다음 지문에서 설명하는 네트워크 기술은?

> 보안 담당자 A씨는 중요 서비스에 대한 방화벽의 이중화 구성 시 방화벽의 링크 상태를 모니터링해 링크가 다운되었을 경우 경로정보를 변경하도록 하는 네트워크 기능을 적용하고자 한다.

① Bypass
② LLCF
❸ Failover
④ DPDK

24. 스니핑 할 수 있는 공격방법과 거리가 먼 것은?

① ARP Redirect
② Switch Jamming
③ ARP Spoofing
❹ IP Spoofing

25. 다음 지문에서 설명하고 있는 공격 특징 및 대응방안과 관련성이 가장 높은 것은?

> 웹서버 OS의 TCP 스택(Stack) 자원을 소모하는 특징을 갖는 웹서버 자원 소모 공격으로 사용될 수 있으며, 그 대응방법으로 Anti-DDoS 장비에서 소스 IP별로 PPS 임계치를 설정하거나 패킷 헤더 검사를 통해 정상적인 옵션 필드값을 갖지 않는 비정상 패킷을 차단할 수 있다.

① UDP Flooding
❷ SYN Flooding
③ ICMP Flooding
④ GET Flooding

26. 컴퓨터 및 네트워크에서 서비스가 더 이상 진행되지 못하도록 하는 경우로써 <보기>에서 설명하고 있는 공격 방법으로 가장 옳은 것은?(관리자 입니다. 문제 복원 오류로 3번 4번 보기가 같습니다. 정확한 내용을 아시는분 께서는 오류 신고를 통하여 내용 작성 부탁 드립니다.)

> - 핑(ping)을 사용하여 현재 동작 중인 노드가 에코 메시지를 보내게 한다.
> - 공격자가 발신주소를 공격하고자 하는 목적지의 IP 주소로 위장하여 ICMP 에코 메시지를 요청하여 다량의 패킷이 목적지로 전송되도록 한다.
> - 목표시스템은 과부하가 발생하여 정상적인 서비스가 불가능 하게 된다.

❶ 스머프(smurf) 공격
② 중간자(man-in-the-middle) 공격
③ 포맷 스트링(format string) 공격
④ 포맷 스트링(format string) 공격

27. 다음 네트워크 공격은 무엇인가?

> 이 공격은 IP 단편화 과정을 이용하는 것으로 공격자가 전송되는 단편 위치 정보(offset)를 조작하여 단편들이 중첩되거나 빈 패킷을 보내는 것처럼 만들어 공격 대상에게 패킷 데이터 재조립 과정을 혼란스럽게 하여 과부하가 걸리게 하는 서비스 거부 공격 기법이다.

① Ping of death
② LAND attack
❸ Teardrop
④ Smurf attack

28. 다음 보기의 내용은 어떤 공격에 대한 특징인가?

> 처음 패킷을 1번으로 보낸 후, 다음 패킷을 100번, 다음 패킷을 200번 등 정상적으로 보내다가 20번째 패킷을 2002, 21번째 패킷을 100, 22번째 패킷을 다시 2002 등으로 중간에 패킷 시퀀스 번호를 비정상적인 상태로 전송하는 공격

① Land Attack
② Bonk
❸ Boink
④ Teardrop

29. 침입차단시스템(Firewall)의 기능과 가장 거리가 먼 것은?

① 로깅(logging)과 감사추적(auditing) 기능
② 네트워크 접근제어 기능
❸ 데이터 축약 기능
④ 사용자 인증 기능

Download on the App Store 전자문제집 CBT(App Store) :[다운로드]
GET IT ON Google Play 전자문제집 CBT(Google Play) :[다운로드]

30. hosts 파일을 통해 도메인 이름에 대한 IP 주소를 적어두면 이 스푸핑 공격에 대응할 수 있다. 이 공격은 무엇인가?

❶ DNS 스푸핑
② IP 스푸핑
③ ARP 스푸핑
④ 이메일 스푸핑

31. 침입차단시스템(Firewall)의 동작 방식은?

- 패킷의 헤더 내용을 분석하여 순서에 위배되는 패킷 차단
- 패킷 필터링 방식에 비해 세션 추적 기능 추가
- 데이터 내부에 악의적인 정보를 포함할 수 있는 프로토콜에 대한 대응이 어려움

① Circuit Gateway
② Application Gateway
③ Packet Filtering
❹ Stateful Inspection

32. 다음에서 설명하고 있는 기술은?

이 기술의 정의는 유동적이나 일반적으로 패킷의 콘텐츠가 담긴 페이로드 부분(Payload)까지 검사할 수 있는 기술로 통용된다. 대규모 네트워크 환경에서 짧은 시간 안에 다양한 애플리케이션을 식별할 수 있는 기술로서 실시간으로 인터넷 트래픽을 분석하여 차별적으로 처리할 수 있도록 진화하였으며, 다양한 기능들을 하나의 장비에 구현할 수 있도록 발전하였다. 이로 인해서 보안, 트래픽 관리, 유해 콘텐츠 차단 등 다양한 목적을 위해 사용될 수 있다.

① ATP
② MPI
❸ DPI
④ SPI

33. 점차 증대되고 고도화되는 보안 위협에 대처하기 위해 예방, 탐지, 대응 등을 위한 보안 도구들을 유기적으로 연결하고 통합함으로써 보안 운영 업무를 자동화하고 보안 운영 효율성 극대화를 도모하는 기술은?

① UTM(Unified Threat Management)
② IDS(Intrusion Detection System)
❸ SOAR(Security Orchestration, Automation and Response)
④ ESM(Enterprise Security Management)

34. Snort의 threshold 옵션에서 다음 지문의 빈칸 ㉠에 들어갈 용어로 알맞은 것은?

60초 내에서 규칙에 매치된 패킷이 200개라면 2번 카운트, 300개라면 3번 카운트
threshold : type (㉠), track by_dst, count 100, seconds 60;

① content
❷ both
③ threshold
④ limit

35. VPN 터널링 프로토콜과 관련이 없는 것은?

① L2TP
② IPSec
③ SOCKS V5
❹ IMAP

36. UTM(Unified Threat Management)에 대한 설명 중 옳지 않은 것은?

① UTM은 다양한 보안 솔루션을 하나의 장비에 탑재하여 운영하는 All-in-One 통합보안 솔루션이다.
❷ 보안정책 적용이 개별적으로 이루어지므로 전문가의 운영이 필요하다.
③ 다양한 보안 기능을 하나의 솔루션에 통합하여 복합 해킹 위협에 효과적으로 대응하는데 목적을 두고 있다.
④ 보안 정책, 필터링 시그니처를 통합 관리하여 일관성과 운영 효율성을 제공한다.

37. TLS Record 프로토콜의 가공 단계를 올바른 순서대로 나열한 것은?

가. Compress 나. Fragment 다. ADD MAC 라. Encrypt 마. Append TLS Record Header

❶ 나 → 가 → 다 → 라 → 마

② 나 → 다 → 가 → 라 → 마

③ 나 → 라 → 다 → 가 → 마

④ 나 → 라 → 가 → 다 → 마

38. 포트 스캔 시 포트가 열린 경우 대상으로부터의 응답이 다른 것은?

❶ TCP Open Scan

② NULL Scan

③ FIN Scan

④ XMAS Scan

39. 빈칸 ㉠, ㉡, ㉢, ㉣에 들어갈 용어들이 올바르게 짝지어진 것은?

- 인증과 무결성을 위해 (㉠) 프로토콜 이용 - 페이로드 기밀성 보호를 위해 (㉡) 프로토콜 이용 - (㉠) 인증값을 계산하기 위해 사용되는 암호 알고리즘은 대칭키 기반의 (㉢) 방식 또는 MD5, SHA 등과 같은 (㉣) 방식을 이용한다.

① ㉠ L2TP ㉡ IPSec ㉢ MAC ㉣ ESP

② ㉠ AH ㉡ IPSec ㉢ Encapsulation ㉣ SSL

❸ ㉠ AH ㉡ ESP ㉢ MAC ㉣ HASH

④ ㉠ L2TP ㉡ IPSec ㉢ HASH ㉣ MAC

40. 보안 솔루션은?

- 접속한 경로와 관계없이 사용자에 대한 인증을 수행 - 사용자의 컴퓨터에 대한 무결성 검사를 수행 (OS 패치 및 구성 정보, 개인 방화벽 유무 등의 검사) - 인증 및 무결성 검사 결과를 정책 관리서버에 설정된 정책과 비교 - 인증 및 무결성 검사 결과를 바탕으로 사용자가 접근하는 대상에 관한 정책 결정을 수행 - 허용, 거부, 격리할 수 있는 일부 적용 장비 유형에 대한 네트워크 액세스 인증을 수행

① IPS

② IDS

③ DLP

❹ NAC

【3과목】 어플리케이션 보안 (20문제)

41. SSH의 기능과 가장 거리가 먼 것은?

① 원격 접속 보호

② 파일 전송 보호

❸ 패킷 필터링

④ 사용자 인증

42. DB 보안 위협 요소인 추론으로부터 정보 유출을 막기 위한 기술은?

① 집성

② DAC

③ 암호화

❹ 다중 인스턴스화

43. 다음 지문의 설명에 가장 알맞은 기술은?

보안 토큰이라고도 이야기하며, 전자 서명 생성키 등 비밀정보를 안전하게 저장, 보관할 수 있고, 기기 내부에 암호 연산 장치가 있어 전자서명키 생성 및 서명 생성 등이 가능한 하드웨어 장치를 말한다.

❶ HSM

② OTP

③ SSO

④ DRM

44. DNS 서버에 대한 질의 시 사용되는 type 옵션에 대한 설명으로 틀린 것은?

① MX : 도메인의 메일서버 질의

② NS : 도메인의 네임서버 질의

③ A : 도메인에 대한 IP 주소 질의

❹ SOA : IP에 대한 도메인 정보 질의

45. 다음 중 HTML 문서 내 입력받은 변수값을 서버측에서 처리할 때 부적절한 명령문이 포함되거나 실행되어 서버의 데이터가 유출되는 취약점은?

❶ SSI 인젝션

② LDAP 인젝션

③ XPATH 인젝션

④ SQL 인젝션

46. 다음 보안 프로토콜 중 작동 레이어가 OSI 7 Layer 중 가장 낮은 것은?

① S/MIME

❷ IPSec

③ SSH

④ SSL

47. 웹 서비스를 주요 대상으로 하는 공격 유형이 아닌 것은?

① CSRF

② XSS

③ RFI

❹ Format String

48. TLS handshake 과정을 순서에 맞게 나열한 것은?

가. Server Key Exchange
나. Server Hello
다. Client Hello
라. Client Key Exchange
마. Change Cipher Spec

① 다 → 라 → 나 → 가 → 마

❷ 다 → 나 → 가 → 라 → 마

③ 다 → 라 → 가 → 나 → 마

④ 다 → 나 → 라 → 마 → 가

49. 다음 중 SQL injection에서 사용되는 여러 종류의 특수문자 용도에 대한 설명으로 가장 적합하지 않은 것은?

❶ -- 및 # 은 앞의 출력값을 받아 두 번째 입력값으로 사용한다.

② ; 은 쿼리 구분 기호이다.

③ ' 은 문자 데이터 구분기호이다.

④ /* */은 구문 주석 처리 기호이다.

50. 디지털포렌식의 일반원칙으로 적합하지 않은 것은?

❶ 증거분석은 원본을 사용하여 분석하여야 한다.

② 디지털 증거는 신뢰성이 검증된 분석 도구(HW, SW)를 사용해야 한다.

③ 디지털 증거는 추출, 분석된 데이터가 무결성, 동일성이 보장되어야 증거능력을 인정받을 수 있다.

④ 증거분석의 전 과정을 기록하여야 한다.

51. 빈칸 ⓐ, ⓑ, ⓒ에 들어갈 상태코드 값으로 알맞은 것은?

클라이언트의 요청이 성공적으로 수신되어 처리되었음을 의미한다. - (ⓐ)번대
서버 자체에서 생긴 오류 상황이나 클라이언트의 요구 사항을 제대로 처리할 수 없을 때 발생한다. - (ⓑ)번대
클라이언트의 요구 사항을 처리하려면 다른 곳에 있는 자원이 필요하다는 것을 의미한다. - (ⓒ) 번대

① ⓐ 200 ⓑ 400 ⓒ 500

② ⓐ 400 ⓑ 300 ⓒ 200

❸ ⓐ 200 ⓑ 500 ⓒ 300

④ ⓐ 300 ⓑ 400 ⓒ 500

52. 전자상거래 보안에서 SSL/TLS의 특징이 아닌 것은?

① SSL은 Record Layer와 Handshake Layer로 구분한다.

② 응용계층의 프로토콜의 안정성을 보장한다.

③ https://* 로 표현된다.

❹ 전자서명을 통한 부인방지를 제공한다.

53. 게시판에 올리는 글에 악성코드를 삽입하여 다른 게시판 이용자가 글을 읽을 경우 악성코드가 실행되도록 하여 클라이언트의 정보를 유출하는 공격 기법에 해당하는 것은?

① File Download

② 쿠키/세션 위조

③ XML 외부 개체

❹ Cross Site Scripting

54. SSL/TLS의 취약점과 관계가 먼 것은?

① Freak

② logjam

③ Poodle

❹ Spectre

55. 다음 지문의 특징을 가진 공격 유형으로 적절한 것은?

- 서버 장악 및 흔적 제거를 위해 PlugX 계열의 악성코드를 주로 사용
- 악성코드 제작자는 제작 단계부터 공격 목표로 삼은 특정 회사를 타깃하여 정밀하게 제작하고 소수의 PC만을 최종적으로 감염시킴으로써 작전을 은밀하게 오래 수행
- 유효한 인증서로 서명된 악성코드 활용, C 런타임 코드 변조 등의 탐지회피 기법에 능하며 고도화되고 지능적으로 공격 수행
- '개발환경 침투'와 '업데이트 서버 침투' 등의 전략 사용

① APT 공격

② 갠드크랩(GandCrab) 공격

③ 클롭(CLOP) 공격

❹ 공급망 공격(Supply Chain)

56. 다음 지문에서 설명하는 웹 공격 기법은?

공격자는 악성코드가 포함된 게시물을 서버에 등록해 두면 로그인된 사용자가 자신의 의지와 무관하게 공격자가 의도한 행위(수정, 삭제, 등록, 송금 등)를 하게 만드는 공격으로서 사용자가 악성 스크립트 구동을 서버에게 요청하여 실제 서버가 실행하도록 한다.

① SQL Injection 공격

② 역직렬화 공격

❸ CSRF 공격

④ 디렉터리 리스팅(Directory Listing) 공격

57. 다음 지문에서 설명하는 것은?

디지털 환경에서 콘텐츠 객체를 식별하기 위한 것으로 고유의 체계에 따라 부여된다. 이를 통해 디지털 콘텐츠의 저작권 보호와 유통 경로 추적이 용이해진다.

① DRM

❷ DOI

③ 스테가노그래피

④ 워터마킹

58. 윈도우 7을 사용하는 사용자가 한국인터넷진흥원 홈페이지(http://www.kisa.or.kr)에 접속하기 위해 IP 주소를 얻어오는 순서로 적절한 것은?

① 로컬 DNS 서버 → 캐시 → Hosts 파일

② Hosts 파일 → 캐시 → 로컬 DNS 서버

③ 로컬 DNS 서버 → Hosts 파일 → 캐시

❹ 캐시 → Hosts 파일 → 로컬 DNS 서버

59. 갑자기 대량의 DNS(Domain Name System) 관련 트래픽이 유입되어 확인해 보니, DNS 증폭공격이라는 것을 알게 되었다. 다음 중 이 공격에 대해 바르게 설명하고 있는 것은?

① DNS zone transfer의 취약점을 이용한 공격이다.

② DNSSEC의 취약점을 이용한 공격이다.

③ DNS bug이므로 취약한 서버는 최신 버전으로 패치를 하여야 한다.

❹ resolving이 허용된 DNS를 매개체로 악용하는 형태의 공격이다.

60. SQL injection 공격 취약점에 대응하기 위한 방법과 가장 거리가 먼 것은?

① 웹 방화벽을 웹 서버 앞단에 두고 미리 필터링 한다.

② 인터프리터 방식을 회피한다.

③ 사용자 입력 값을 모두 Encoding 하여 유효성을 검증한다.

❹ 현재 쓰고 있는 웹브라우저를 업그레이드 하거나, 다른 것으로 바꾼다.

【4과목】 정보 보안 일반 (20문제)

61. 다음 지문에서 설명하는 정보보호 용어는?

> 조직이나 시스템에 손실 또는 손해를 유발시킬 수 있는 사항들의 집합으로 정의된다. 예로는 해킹, 악성코드, 파손 행위, 화재 등을 들 수 있다.

❶ 위협(threat)
② 취약점(vulnerability)
③ 자산(asset)
④ 위험(risk)

62. 다음 지문에서 설명하고 있는 원칙은?

> - 개발자는 운영 데이터에 접근할 수 없으나 테스트를 위해 관리자의 승인을 받을 경우 제한된 규모의 운영 데이터에 접근할 수 있다.
> - 서버 관리자는 시스템 로그에 접근할 수 없다.

① 직무 순환
② 상호 배제
③ 책임추적성 보장
❹ 직무 분리

63. 다음 지문은 블록 암호 알고리즘을 분석하는 방법에 대한 서술이다. 이 분석법에서 사용한 암호 해독의 원리는?

> 먼저 암호 알고리즘의 비선형 요소에 대해 평문의 차분과 암호문의 차분 사이의 관계에 대한 차분 분포표를 구성한다. 그 후 차분 분포표에서 높은 확률을 갖는 공격에 필요한 평문 목록을 구성하고, 암호문을 선택하고 그에 대응하는 평문을 얻어 키의 특정 비트 정보를 찾는다.

① 암호문 단독 공격
② 선택 평문 공격
③ 알려진 평문 공격
❹ 선택 암호문 공격

64. 전체 사용자가 10명인 시스템(또는 조직)내에서 어떤 사용자가 다른 사람에게 암호화된 메시지를 대칭키 암호를 사용하여 교환하고자 한다. 이때, 서로 다른 2명씩 대칭키를 사전에 공유한다고 가정할 때, 전체 시스템에서 존재하는 서로 다른 대칭키의 개수는 몇 개인가?

① 10
❷ 45
③ 55
④ 100

65. 기존의 사람과 사람, 사람과 디바이스 중심의 네트워크 환경이 디바이스와 디바이스 간의 네트워크로 확장됨에 따라 디바이스 인증이 중요한 쟁점으로 부각되고 있다. 디바이스 인증에 대한 설명 중 틀린 것은?

① 디바이스의 진위성 및 네트워크 접속 권한을 제어하기 위한 것이다.
② 비 인가된 디바이스가 네트워크에 접속되어 IT 서비스를 위협하는 것을 방지하기 위한 것이다.
③ 네트워크에 참여하는 다양한 디바이스들을 신뢰할 수 있도록 하기위한 것이다.
❹ 네트워크 및 시스템 사용권을 허가된 사용자로 제한하기 위한 것이다.

66. SSO(Single Sign On)는 사용자가 단 한 번의 인증절차만으로 다수의 애플리케이션에 접속할 수 있도록 해주는 인증 프로세스로 인증시간 단축, 사용자 계정의 효율적 관리, 접근권한의 효율적 통제가 가능하다. 다음 중 SSO 방식과 가장 거리가 먼 것은?

❶ RADIUS
② SPNEGO
③ Kerberos
④ SESAME

67. 대칭키 암호화와 MAC(Message Authentication Code)으로 해결할 수 없는 보안서비스는?

① 메시지 무결성(Integrity)
② 메시지 인증(Authentication)
❸ 메시지 부인방지(Non Repudiation)
④ 메시지 기밀성(Confidentiality)

68. 다음 중 MD 계열 해시함수의 특징으로 옳지 않은 것은?

❶ 160Bit의 출력 해시값을 생성한다.
② 데이터 무결성을 위해 메시지 압축 · 축약을 하는 해시 알고리즘이다.
③ 해시 충돌 방지 확률은 약 이다.
④ MD4의 경우, 속도가 빠른 반면에 안정성에서 뒤떨어진다.

69. 다음 지문에서 설명하는 접근통제 모델은?

> 이 모델은 객체에 대한 소유권을 기반으로 소유권을 갖는 주체가 객체에 대한 권한의 일부 또는 전부를 다른 주체에게 부여할 수 있다.

① 강제적 접근통제 모델
② 규칙기반 접근통제 모델
③ 역할기반 접근통제 모델
❹ 임의적 접근통제 모델

70. 다음은 암호키 관리의 운영단계 중 키변경 기능(Key Change Function)에 대한 설명이다. 잘못된 것은?

① 기존의 암호키를 이용하여 새로운 암호키를 생성하는 방법을 키 갱신이라고 한다.
② 기존의 암호키와는 독립적인 방법으로 새로운 암호키를 생성하는 방법을 키 교체라고 한다.
❸ 갱신된 암호키가 노출된 경우, 갱신되기 이전의 암호키에 대한 정보는 노출되지 않으므로, 기존의 암호키가 노출되면 노출된 암호키를 변경하기 위해 키 갱신을 사용한다.
④ 암호키의 노출이 확인되거나, 노출의 위협이 있는 경우 혹은 암호키 유효 기간의 만료가 가까워지는 경우 암호키를 안전하게 변경해야 하며, 암호키를 변경한 이후에는 기존의 암호키를 정지단계로 전환해야 한다.

71. 다음 중 역할기반 접근통제(Role Based Access Control)의 설명으로 틀린 것은?

① 대개 구현을 위하여 역할에 대한 추상화 작업이 요구된다.
② Non-DAC 또는 비임의적 접근통제 모델로도 불린다.
③ 사용자의 역할 및 직능에 따라 접근을 통제하는 방식이다.
❹ 사용자에게 지나친 권한이 부여될 우려가 있다.

72. Kerberos 프로토콜이 적용된 시스템에 대한 설명 중 틀린 것은?

① 사용자, 클라이언트, 인증서버, 티켓발급 서버, 응용서버로 구성된다.
② 인증된 클라이언트만 서버에 접근하도록 고안된 보안시스템이다.
③ 인증 혹은 티켓 발급 서버가 정지되면 전체 서비스가 중단된다.
❹ 데이터의 무결성, 기밀성, 가용성, 부인방지 등의 보안 서비스를 제공한다.

73. 다음 지문에서와 같이 정의되었을 때, A가 B에게 메시지 M을 암호화 하여 보내고자 한다. 올바른 설명은?(문제 오류로 보기 내용이 정확하기 않습니다. 정확한 보기 내용을 아시는분 께서는 오류 신고를 통하여 내용 작성 부탁 드립니다. 정답은 3번 입니다.)

> ( ) : A의 개인키(Apri)와 공개키(Apub) 쌍
> ( ) : B의 개인키(Bpri)와 공개키(Bpub) 쌍
> : 키 로 암호화 표기
> : 키 로 복호화 표기
> : 평문 메시지
> : 암호문 메시지

① 1
② 1
❸ 1
④ 1

74. X.509 확장 영역에 속하는 것은?

① 공개키
② 서명 알고리즘
③ 인증서의 버전
❹ 주체 키 식별자

75. ⓐ, ⓑ 각각이 설명하는 서명 방식은 무엇인가?

> ⓐ 사용자 A가 서명자 B에게 자신의 메시지(서명문)를 보여주지 않고 서명자가 서명하는 방식으로 서명을 받는 사람의 신원과 서명문을 연결시킬 수 없도록 익명성을 제공하는 서명방식으로 메시지의 비밀성을 지키면서 타인의 인증을 받고자 하는 경우 사용됨.
> ⓑ 전자상거래에서 구매자는 해당 주문에 대해 지불 정보와 주문 정보에 대해 각각의 해시값을 구하고, 두 해시를 합해 다시 한 번 해시값을 구하여 구매자가 마지막 해시값을 자신의 개인키로 서명하는 방식임.

① ⓐ 이중서명 ⓑ 정규서명
② ⓐ 이중서명 ⓑ 분할서명
③ ⓐ 은닉서명 ⓑ 분할서명
❹ ⓐ 은닉서명 ⓑ 이중서명

76. 이론적으로 전수공격(Brute Force Attack)에 가장 강한 암호 기법은?

① RC4
② 3-DES
③ AES
❹ OTP(One Time Pad)

77. 메시지 인증을 위해 송신자가 메시지와 이에 대한 MAC 값을 동시에 수신자에게 보낼 때, 중간 공격자가 이를 가로채 가지고 있다가 송신자를 가장하여 언제든 수신자에게 보내는 재전송 공격이 가능하다. 다음 중 이를 방어하는 기술이 아닌 것은?

① 메시지를 보낼 때 마다 순서번호(Sequence Number)를 포함시켜 MAC 값을 계산한다.
② 메시지를 보낼 때 마다 순서번호(Sequence Number)를 포함시켜 MAC 값을 계산한다.
③ 비표(Nonce) 값을 포함시켜 MAC 값을 계산한다.
❹ MAC 값을 암호화한다.

78. Kerberos 키 분배 프로토콜의 기반 기술에 해당하는 것은?

❶ Needham-Schroeder 프로토콜
② Diffie-Hellman 프로토콜
③ Challenge-Response 프로토콜
④ RSA 이용 키 분배 프로토콜

79. 다음 지문에서 설명하고 있는 대칭키 암호 알고리즘은?

128비트의 키를 사용하여 64비트의 평문을 8라운드를 걸쳐 64비트 암호문으로 만든다. 모든 연산이 16비트 단위로 이루어지도록 하여 16비트 프로세서에서 구현이 용이한 암호알고리즘이다.

① SEED
② DES
③ SHA-1
❹ IDEA

80. 다음 지문은 공개키 암호방식에 대한 내용을 설명한 것이다. (가)~(마)에 들어가야 할 단어로 옳은 것은?

두 개의 (가) p, q를 선택하여 n = (나)를 계산한다. 이때, p, q를 알고 있는 사람은 n을 계산하기 쉽지만, n만 알고 있는 사람은 n으로부터 p, q를 찾는 것은 어렵다. 이를 (다)라고 한다. 이에 기반한 대표적인 공개키 암호 알고리즘은 (라), (마)이다.

① (가) 정수 (나) p × q (다) 이산대수 문제 (라) RSA (마) ElGamal
② (가) 소수 (나) p + q (다) 소인수분해 문제 (라) 타원곡선 암호 (마) Diffie-Hellman 암호
③ (가) 실수 (나) p + q (다) 이산대수 문제 (라) Rabin 암호 (마) 타원곡선암호
❹ (가) 소수 (나) p × q (다) 소인수분해 문제 (라) RSA (마) Rabin 암호

【5과목】 정보보안 관리 및 법규 (20문제)

81. 과학기술정보통신부장관은 다음 중 어느 하나에 해당하는 사유를 발견한 경우 정보보호 관리체계 인증을 취소할 수 있다. 해당 사유 발생 시 반드시 인증을 취소해야 하는 것은?

❶ 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증을 받은 경우
② 사후관리를 거부한 경우
③ (과학기술정보통신부장관이 정한 인증기준에 미달하게 된 경우
④ 사후관리를 방해한 경우

82. 개인정보의 안정성 확보조치 기준(고시)의 제7조(개인정보의 암호화)에 따라 반드시 암호화하여 저장해야하는 개인정보가 아닌 것은?

① 비밀번호
② 고유식별번호
③ 바이오 정보
❹ 전화번호

83. 아래 지문에서 설명하고 있는 것은 무엇인가?

> 모든 정보시스템에 대하여 표준화된 보안 대책을 제시하며 Check List로 보안대책이 있는지 판단한다. 즉 적용되지 않은 보안대책을 확인하는 위험분석 방법이다.

① 정성적 위험분석
② 정량적 위험분석
③ 상세 위험분석
❹ 베이스라인 접근법

84. 정보보호 내부 감사 시 고려해야할 사항으로 가장 부적합한 것은?

❶ 내부감사를 수행하는 구성원은 정보보호 전문가들로 제한한다.
② 감사의 범위는 다양한 위험을 분석 및 검토할 수 있도록 가능한 포괄적이어야 한다.
③ 감사활동은 기업 내외부로부터 독립성을 유지할 수 있도록 해야 한다.
④ 내부감사는 조직의 위험을 파악하여 개선사항을 제시할 수 있다.

85. 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업의 내부관리계획의 내용에 포함하지 않아도 될 사항은 무엇인가?

① 개인정보 보호책임자의 지정에 관한 사항
② 개인정보 유출사고 대응 · 계획 수립 · 시행에 관한 사항
③ 개인정보의 암호화 조치에 관한 사항
❹ 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항

86. 다음 중 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 47조의 정보보호 관리체계의 인증 제도에 대한 설명으로 옳지 않은 것은?

① 정보보호 관리체계 인증의 유효기간은 3년이다.
② 정보보호 관리체계 인증은 의무 대상자는 반드시 인증을 받아야 하며 의무 대상자가 아닌 경우에도 인증을 취득할 수 있다.
③ 정보보호 관리체계는 정보통신망의 안정성 · 신뢰성 확보를 위하여 관리적 · 기술적 · 물리적 보호조치를 포함한 종합적 관리체계를 의미한다.
❹ 정보보호 관리체계 의무대상자는 국제표준 정보보호 인증을 받거나 정보보호 조치를 취한 경우에는 인증 심사의 전부를 생략할 수 있다.

87. 개인정보처리자가 정보주체의 동의를 받을 때 정보주체에게 알려야 하는 항목이 아닌 것은?

① 개인정보의 수집 · 이용 목적
② 수집하려는 개인정보의 항목
③ 개인정보의 보유 및 이용 기간
❹ 개인정보의 수집 출처

88. 정성적 위험분석 방법론에 해당되지 않는 것은?

① 델파이 기법
② 순위 결정법
③ 시나리오법
❹ 과거 자료 분석법

89. 다음 중 아래 내용에 해당하는 위험분석 방법론으로 적절히 짝지은 것은?

> ㉠ 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정 조건하에서 위협에 대한 발생 가능한 결과들을 추정하는 방법
> ㉡ 각각의 위협을 상호 비교하여 최종 위협요인의 우선순위를 도출하는 방법

① ㉠ 시나리오법 ㉡ 델파이법
② ㉠ 확률 분포법 ㉡ 순위결정법
③ ㉠ 델파이법 ㉡ 확률 분포법
❹ ㉠ 시나리오법 ㉡ 순위결정법

90. 다음의 ISMS 인증 의무 대상자에 대한 설명으로 잘못 기술 된 것은?

① 전기통신사업법의 전기통신사업자로 전국적으로 정보통신망 서비스를 제공하는 사업자
② 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영 · 관리하는 사업자
③ 정보통신서비스 부문 전년도 매출액 100억 이상 사업자
❹ 전년도말 기준 직전 6월간 일일 평균 이용자 수 100만명 이상 사업자

91. 다음 경제협력개발기구(OECD) 개인정보 보안 8원칙에 대한 설명 중 옳지 않은 것은?

① 수집 제한의 법칙: 개인정보는 적법하고 공정한 방법을 통해 수집해야 한다.

② 목적 명시의 원칙(Purpose Specification Principle): 개인정보는 수집 과정에서 수집 목적을 명시하고, 명시된 목적에 적합하게 이용해야 한다.

❸ 비공개의 원칙(Closedness Principle): 개인정보의 처리 및 보호를 위한 관리자에 대한 정보는 비공개해야 한다.

④ 책임의 원칙(Accountability Principle): 개인정보 관리자에게 원칙 준수 의무 및 책임을 부과해야 한다.

92. 다음 중 위험분석을 위한 ALE 계산에 사용되지 않는 값은 무엇인가?

① 자산가치

② 노출계수

③ 연간발생률

❹ 우선순위

93. 정보시스템의 개발 및 시험 과정을 검토한 결과, 정보보안측면에서 가장 적절하지 않은 것은?

① 시험데이터로 임의의 데이터를 생성하거나 운영데이터를 가공 변환한 후 사용하고 있다.

② 실 운영데이터를 테스트 용도로 사용하고 테스트 완료 후 테스트 DB에서 삭제하였다.

❸ 이전 버전의 소스 코드를 운영 서버에 보관하고 있다.

④ 실 운영데이터를 테스트 용도로 사용하고 테스트 DB에 대해 운영 DB와 동일한 수준의 접근통제를 적용하고 있다.

94. 다음 지문에서 설명하는 백업 설비는?

> 주 센터와 동일한 수준의 정보기술자원을 대기상태(Standby)로 원격지 사이트에 보유하면서 (Active-Standby), 주 센터 재해 시 원격지 시스템을 Active 상태로 전환하여 서비스를 제공한다.

① 콜드 사이트

② 미러 사이트

③ 웜 사이트

❹ 핫 사이트

95. 다음 빈칸 ㉠에 들어갈 말로 적절한 것은?

> (㉠)은 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도이다. 인증범위로는 정보서비스의 운영 및 보호에 필요한 조직, 물리적 위치, 정보자산 뿐만 아니라 개인정보처리를 위한 수집, 보유, 이용, 제공, 파기에 관여하는 개인정보처리 시스템, 취급자를 포함한다.

① ISMS

② PIMS

❸ ISMS-P

④ GDPR

96. 다음 지문의 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서 정의하는 용어에 대한 설명으로 옳지 않은 것은 무엇인가?

> a. "전자문서"란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 암호화되어 저장된 문서형식의 자료로서 표준화된 것을 말한다.
>
> b. "개인정보"란 생존 및 사망한 개인에 관한 정보로서 성명 · 주민등록번호 등에 의하여 특정한 계정을 알아볼 수 있는 부호 · 문자 · 음성 · 음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
>
> c. "침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.
>
> d. "이용자"란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.

❶ a, b

② b, c

③ c, d

④ b, d

97. 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 따라 침해사고의 유형별 통계, 해당 정보 통신망의 소통량 통계 및 접속경로별 이용 통계 등의 침해사고 관련 정보를 과학기술정보통신부 장관이나 한국인터넷진흥원에 제공해야 하는 기관이 아닌 것은?

❶ 정보보호 전문서비스 기업

② 주요정보통신서비스 제공자

③ 컴퓨터바이러스 백신소프트웨어 제조자

④ 집적정보통신시설 사업자

98. 다음에서 설명하는 것은?

> 정보통신서비스 제공자는 새로이 정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 때에는 그 계획 또는 설계에 정보보호에 관한 사항을 고려하여야 한다.
> IT 서비스의 구축 단계에서 정보보호 위협 및 취약점 분석·위험분석 등의 절차를 통해 사전에 취약점을 제거하고 보호대책을 수립하는 일련의 보안 컨설팅 활동이다.

① 암호모듈검증 제도

② 정보보호시스템 공통평가 제도

③ 보안 적합성 검증 제도

❹ 정보보호 사전점검 제도

99. 위험 분석 수행의 주목적은 기업이 피해를 입었을 때 손실 비용에 대한 값을 산정하거나 가치를 부여하기 위해 잠재적 위협의 충격 정도를 정하는 것이다. 위협이 가해질 때 특정 위협이나 위협 그룹에 관련된 위험을 제거하기 위해 적용된 통제나 대응방안을 의미하는 것은?

❶ 세이프가드

② 규제 정책

③ 가이드

④ 복구 절차

100. 정보보호 관리의 목적, 이유, 범위 등에 대한 거시적이고 개괄적인 설명 중 가장 부적절한 것은?

① 조직은 정보보호관리를 통해 정보 및 자산의 기밀성, 무결성, 가용성 서비스를 받을 수 있다.

② 조직이 정보보호관리를 구현하고 실행하는 것은 조직의 목적, 보안요구사항, 조직의 크기 및 구조에 영향을 받는다.

③ 조직의 요구 및 수요에 따라 정보보호관리 규모가 변화될 수 있다.

❹ 정보보호관리의 적용 범위는 정보보호 실무자가 위험분석에 의해 결정한다.